



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,367	01/31/2002	Robert David Zobel	05456.105009	2476
7590	03/07/2006			
Robert T. Neufeld, Esq. KING & SPALDING 45th Floor 191 Peachtree Street, N.E. Atlanta, GA 30303			EXAMINER SHAW, YIN CHEN	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

1. This written action is responding to the amendment dated 12/14/2005.
2. Claims 1, 5, 13, 17, 21, 22, 24, 30, 33, 39, 40, 42, and 44 have been amended while Claims 14, 28, and 37 have been cancelled. Claims 2-4, 6-12, 15-16, 18-20, 23, 25-27, 29, 31-32, 34-36, 38, 41, 43, and 45 have been kept as original.
3. Claims 1-45 have been submitted for examination.
4. Claims 1-45 have been examined and rejected.

Priority

5. The application has been filed under Title 35 U.S.C. 119(e), claiming priority to provisional application 60/265,519, filed on Jan. 31, 2001.
6. The effective filing data for the subject matter defined in the pending claims in this application is Jan. 31, 2001.

Information Disclosure Statement

7. The Information Disclosure Statement dated on Oct. 11, 2005 contains numerous duplicated patent, publication, and non-patent information entries that are either being previously disclosed by the Applicant or the Office. Therefore, these entries have been crossed out and are not being considered by the Office again.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 30, 32, 34-35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and further in view of Gleichauf et al. (U.S. Patent 6,301,668) and Kingsford et al. (U.S. Patent 6,574,737).

a. Referring to Claim 30:

As per Claim 30, Proctor discloses a method for assessing the security of a network comprising the steps of:

selecting an audit scan to perform on the network element, said selection based on the initial scan [i.e., **Object audit 324 can include an identification of one or more objects 322 to which the audit pertains, a user or users 326 whose activities should be audited with respect to identified objects, and operations 328 performed or attempted on the identified object or objects (lines 56-61, Col 7).** Registry key audit 334 can include an identification of a list 332 of one or more registry keys to be audited, a user or user 336 whose activities should be audited, a user or user 336 whose activities should be audited with respect to identified files, and operations

338 performed or attempted on the identified registry keys (lines 63-67, Col. 7). One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)];

performing the selected audit scan on the network [i.e., The auditing performed can include monitoring the networked computing environment for the occurrence of the identified activities for the users or groups of users (lines 10-12, Col. 2)].

receiving data from the selected audit scan of the network element [i.e., Collection policies are policies that set forth the specific details on how or when the auditing information is to be collected (lines 29-30, Col. 9)]; and

computing a security score for the network element from the selected audit scan [i.e., In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach,

attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system. The security policy can define parameters such as, for example, minimum and maximum password age, minimum and maximum password length, password uniqueness, account lockout, reset account time frames, lockout durations, forced log outs, user log ons to change password, and other security policies (lines 12-18, Col. 10). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11); *where the security value sets the threshold value, which is used in comparing with the security assessment result (security score) to determine whether a breach occurs or will occur*].

Proctor does not expressly disclose the remaining limitations of the claim. However, Gleichauf et al. disclose receiving an initial scan identifying a network element [i.e., Scan engine 22 can direct requests

upon the network and assess responses to such request to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices and the services available on each device (lines 59-62, Col. 5)].

Proctor and Gleichauf et al., Kingsford et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to have a scanning system capable of providing different scope of scanning functions by combining the network scan from Gleichauf et al. with the object and registry scans from Proctor and the detailed vulnerabilities values disclosed in Kingsford associated with the security assessment from Proctor since one would have been motivated to (1) have a security product function in an environment wherein the traffic exceeds their memory or processor capacity (lines 34-36, Col. 2 from Gleichauf et al.) and (2) have information contained in the data record reveals a security vulnerability discovered by the module (lines 39-41, Col. 19 from Kingsford et al.). Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Kingsford to obtain the invention as specified in Claim 30.

b. Referring to Claim 32:

As per Claim 32, Proctor, Gleichauf et al., and Kingsford et al. disclose the method of claim 30. In addition, Proctor discloses modifying the selected audit scan, said modification based on the data received from the selected audit scan [i.e., **The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 41-45, Col. 11). When security assessment 924 determines that an actual attempted or potential security breach has occurred or is occurring, one or more policy updates 928 are made to on or more of the audit policy 904, collection policy 912, and detection policy 916 (lines 49-53, Col. 11)].**

c. Referring to Claim 34:

As per Claim 34, it encompasses limitations that are similar to those of Claim 30. Thus, it is rejected with the same rationale applied against Claim 30 above.

d. Referring to Claim 35:

As per Claim 35, Proctor, Gleichauf et al., and Kingsford et al. disclose the method of claim 30, wherein the step of selecting an audit scan is based on a manual input [i.e., **One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8**

from Proctor), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9 from Proctor)].

e. Referring to Claim 38:

As per Claim 38, Proctor, Gleichauf et al., and Kingsford et al. disclose the steps recited in claim 30. In addition, Proctor discloses a computer-readable medium having computer-executable instructions [i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)].

9. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Kingsford et al. (U.S. Patent 6,574,737) as applied to claim 30 above, and further in view of Hartley et al. (U.S. Patent 6,889,168).

a. Referring to Claim 31:

As per Claim 31, Proctor, Gleichauf et al., and Kingsford disclose the method of claim 30. Proctor, Gleichauf et al., and Kingsford et al. do not expressly disclose the step of scheduling the selected audit scan, said scheduling based on the initial scan. However, Hartley et al. disclose the scheduling module which is used for specifying the time of conducting security modules or all the test [i.e., **The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14, Col. 7). A variety of further screens may be presented which provide the system user the choices of one or more modules scheduled, the data which the function will be performed. Further options may be provided such as periodic activation of the functions, one time activations of the functions, or the combination of various security and utility modules (lines 31-38, Col. 10)].** Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor, Gleichauf et al. and Kingsford et al. with

Hartley et al. to have the initial scan scheduled prior to the audit scan since one would be motivated to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.). Therefore, it would have been obvious to modify Proctor, Gleichauf et al., and Kingsford et al. with Hartley et al. to obtain the invention as specified in Claim 31.

10. Claims 1-2, 4-5, 9, 11-13, 15, 17, 20-23, 25-26, 29, 39, 42-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and further in view of Gleichauf et al. (U.S. Patent 6,301,668), Kingsford et al. (U.S. Patent 6,574,737), and Hartley et al. (U.S. Patent 6,889,168).

a. Referring to Claim 1:

As per Claim 1, Proctor discloses a computer-implemented method for configuring a security audit of a computer network **[i.e., a networked computing environment (line 67, Col. 4)]** comprising the steps of: configuring an audit scan to perform on the element, wherein the audit scan is a more thorough scan than the element **[i.e., Object audit 324 can include an identification of one or more objects 322 to which the audit pertains, a user or users 326 whose activities should be audited with respect to identified objects, and operations 328 performed or attempted on the identified object or objects (lines 56-61, Col 7). Registry key audit 334 can include an identification of a**

list 332 of one or more registry keys to be audited, a user or user 336 whose activities should be audited, a user or user 336 whose activities should be audited with respect to identified files, and operations 338 performed or attempted on the identified registry keys (lines 63-67, Col. 7). One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)];

calculating a security score for the element based on the audit scan [i.e., In one embodiment, the detection policy is used to establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system. The security policy can define parameters such as, for example, minimum and maximum password age, minimum and

maximum password length, password uniqueness, account lockout, reset account time frames, lockout durations, forced log outs, user log ons to change password, and other security policies (lines 12-18, Col. 10). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11); *where the security value sets the threshold value, which is used in comparing with the security assessment result (security score) to determine whether a breach occurs or will occur]*

Proctor discloses performing the audit scan on the element [i.e., The auditing performed can include monitoring the networked computing environment for the occurrence of the identified activities for the users or groups of users (lines 10-12, Col. 2)].

Proctor does not expressly disclose the remaining limitations of the claim. However, Gleichauf et al. disclose conducting a discovery scan to identify an element of the computer network and determine the element's functions [i.e., Scan engine 22 can direct requests upon

the network and assess responses to such request to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices and the services available on each device (lines 59-62, Col. 5)] and scanning process can be repeated [i.e., At step 124 it is determined if the scanning steps should be repeated. If so, the method returns to step 100 to obtain updated network information, and the method is repeated (lines 12-14, Col. 9)]. In addition, Kingsford et al. disclose by summing one or more vulnerabilities associated with the network element [In the preferred embodiment, vulnerabilities are assigned a risk value on a scale of 1-100, with 1-33 being low risk, 34-66 being medium risk, and 67-100 being high risk. Each system's risk and/or collective risk profile for the penetration test can be displayed to the user on the user interface (lines 41-46, Col. 19)], and Hartley et al. disclose the scheduling module which is used for specifying the time of conducting security modules or all the test based on the choices [i.e., The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14,

Col. 7). A variety of further screens may be presented which provide the system user the choices of one or more modules scheduled, the data which the function will be performed. Further options may be provided such as periodic activation of the functions, one time activations of the functions, or the combination of various security and utility modules (lines31-38, Col. 10)].

Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with (1) Gleichauf et al. to have the different scope of scanning capability for the system, (2) Kingsford et al. to have the vulnerabilities values associated with the security assessment result, such as the security score, and (3) Hartley et al. to have scheduling a time to perform the audit scan on the element, scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan and security assessment result, such as the security score. The motivation for doing so would be to have a security product (1) function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.), (2) have information contained in the data record reveals a security vulnerability discovered by the module

(lines 39-41, Col. 19 from Kingsford et al.), and (3) protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.). Therefore, it would have been obvious to modify Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to obtain the invention as specified in Claim 1.

b. Referring to Claim 2:

As per Claim 2, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. In addition, Proctor discloses the step of configuring a subsequent audit scan of the element that is different from the audit scan [i.e., **One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8), where the type of object audit can be subjected to variety of edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9).**]

c. Referring to Claim 4:

As per Claim 4, the rejection of Claim 1 is incorporated. In addition, Claim 4 encompasses the same limitations that are similar to those of

Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

d. Referring to Claim 5:

As per Claim 5, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. In addition, Gleichauf et al. disclose wherein the step of conducting a discovery scan further comprises identifying the one or more vulnerabilities associated with the element **[i.e., In step 108, the potential vulnerabilities discovered in step 106 are confirmed, for example by executing active exploits on the network against the potential vulnerabilities (lines 15-18, Col. 8)].**

e. Referring to Claim 9:

As per Claim 9, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. do not expressly disclose wherein the step of configuring an audit scan comprises selecting a type of audit scan based on the discovery scan. However, Proctor discloses configuring an audit scan as in Claim 1. In addition, Gleichauf et al. disclose the discovery scan as in Claim 1. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. to have an audit scan

process selected based on the prior discovery scan since one would have been motivated to **have a increased security measure as users became more sophisticated (lines 36 and 43, Col 1)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to obtain the invention as specified in Claim 9.

f. Referring to Claim 11:

As per Claim 11, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. In addition, Proctor discloses wherein the step of configuring an audit scan comprises manually selecting the type of audit scan **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8), where the type of object audit can be subjected to variety of edition and modification. Although the functionality is not illustrated on the screen diagram of FIG. 5, the functionality can be provided in one embodiment to allow the administrator to create and edit custom groups (lines 50-53, Col. 8). FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7,**

Col. 9). Additionally, the administrator can select whether to replace auditing on existing sub keys as illustrated by selection box 614 (lines 16-18, Col 9)].

g. Referring to Claim 12:

As per Claim 12, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the steps recited in claim 1. In addition, Proctor discloses a computer-readable medium having computer-executable instructions [i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)].

h. Referring to Claim 13:

As per Claim 13, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

i. Referring to Claim 15:

As per Claim 15, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

j. Referring to Claim 17:

As per Claim 17, the rejection of Claim 13 is incorporated. In addition, Claim 17 encompasses limitations that are similar to those of Claim 4

and 5. Thus, it is rejected with the same rationale applied against Claim 4 and 5 above.

k. Referring to Claim 20:

As per Claim 20, the rejection of Claim 13 is incorporated. In addition, Claim 20 encompasses limitations that are similar to those of Claim 11. Thus, it is rejected with the same rationale applied against Claim 11 above.

l. Referring to Claim 21:

As per Claim 21, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the steps recited in claim 13. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)].**

m. Referring to Claim 22:

As per Claim 22, it encompasses limitations that are similar to those of Claim 1 and 30. Thus, it is rejected with the same rationale applied against Claim 1 and 30 above.

n. Referring to Claim 23:

As per Claim 23, the rejection of Claim 22 is incorporated. In addition, Claim 23 encompasses limitations that are similar to those of Claim 32.

Thus, it is rejected with the same rationale applied against Claim 32 above.

o. Referring to Claim 25:

As per Claim 25, it encompasses limitations that are similar to those of Claim 22. Thus, it is rejected with the same rationale applied against Claim 22 above.

p. Referring to Claim 26:

As per Claim 26, the rejection of Claim 22 is incorporated. In addition, Claim 26 encompasses limitations that are similar to those of Claim 35. Thus, it is rejected with the same rationale applied against Claim 35 above.

q. Referring to Claim 29:

As per Claim 29, Proctor, Gleichauf et al., and Hartley et al. disclose the steps recited in claim 22. In addition, Proctor discloses a computer-readable medium having computer-executable instructions [i.e., **FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17))**].

r. Referring to Claim 39:

As per Claim 39, Proctor discloses a system for configuring [i.e., **One example implementation of creating an object audit is illustrated n**

FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)] a security audit of a computer network comprising the computer network [i.e., a computer network (line 3, Col. 5)]. Proctor further discloses a console operable for receiving and transmitting information about the audit scan [i.e., Security procedures can also be applied to security console 104B (lines 42-43, Col. 5). In one embodiment, the security procedures can include for example, one or more of security policies, collection policies, detection policies and audit policies. The security console 104B can also perform the adaptive feedback operations, including updating the security procedures based on security occurrences (lines 45-47, Col. 5). The example embodiment illustrated in FIG. 3, the audit policy 300 includes a system audit 304, and object audit 324, and a registry key audit 334 (lines 48-50, Col. 7)]. Proctor further discloses computing a security score for the network element from the selected audit scan [i.e., In one embodiment, the detection policy is used to

establish thresholds or limits which, when reached, trigger an alarm or other condition indicating that a security breach, attempted security breach, or other network security condition has occurred or is occurring (line 67, Col. 9 and lines 1-4, Col. 10). The security policy can include security settings or values, which define the security of the system. The security policy can define parameters such as, for example, minimum and maximum password age, minimum and maximum password length, password uniqueness, account lockout, reset account time frames, lockout durations, forced log outs, user log ons to change password, and other security policies (lines 12-18, Col. 10). The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908. The security assessment is performed in accordance with the detection policy or policies 916 established for the network, or for that user or workstation (lines 41-48, Col. 11); *where the security value sets the threshold value, which is used in comparing with the security assessment result (security score) to determine whether a breach occurs or will occur*]. Proctor does not expressly disclose a discovery scan and scheduling feature associated with different types of scans,

However, Gleichauf et al. disclose a security audit system **[i.e., network security system 20 (line 16, Col. 5)]** operable for conducting a discovery scan to identify an element of the computer network **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5)]**. In addition, Kingsford et al. disclose by summing one or more vulnerabilities associated with the network element **[In the preferred embodiment, vulnerabilities are assigned a risk value on a scale of 1-100, with 1-33 being low risk, 34-66 being medium risk, and 67-100 being high risk. Each system's risk and/or collective risk profile for the penetration test can be displayed to the user on the user interface (lines 41-46, Col. 19)]**, and Hartley disclose the scheduling module which is used for specifying the time of conducting security modules or all the test **[i.e., The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14, Col. 7)]**. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary

skill in the art at the time of invention was made to combine Proctor with (1) Gleichauf et al. to have the scanning process performed at different scope for the system by communicating through the console, (2) Kingsford et al. to have the vulnerabilities values associated with the security assessment result, such as the security score, and (3) Hartley et al. to have a system with scheduling feature for the audit scan a time to perform the audit scan on the element, (1) function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.), (2) have information contained in the data record reveals a security vulnerability discovered by the module (lines 39-41, Col. 19 from Kingsford et al.), and (3) protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.). Therefore, it would have been obvious to modify Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to obtain the invention as specified in Claim 39.

s. Referring to Claim 42:

As per Claim 42, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises a system scanning engine operable for detecting particular one of the vulnerabilities on the network element [i.e., **Additionally, in the embodiment of FIG. 1, scan engine 22 is operable to analyze the network information to identify**

potential vulnerabilities of internal network 10 (lines 62-65, Col. 15)].

t. Referring to Claim 43:

As per Claim 43, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises an Internet scanning engine operable for performing a discovery scan on the network [i.e., **Scan engine 22 can direct request upon the network and assess responses to such requests to discover network information. In one embodiment, scan engine 22 scans devices on internal network, such as workstations 12. For example, Scan engine 22 could ping devices on internal network 10 and then perform port scans on each device. Banners from the port scans could be collected and analyzed to discover network information (lines 52-59, Col. 5)].**

u. Referring to Claim 44:

As per Claim 44, Proctor, Gleichauf et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose the security audit system. Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Hartley et al. disclose a database scanning engine operable for detecting vulnerabilities associated with database elements within the network [i.e., **The integrity checker**

module 22 performs an analysis of the computer system in order to find security holes located therein. The analysis performed may find vulnerabilities in such things as: the type of computer/operating system used, the access privileges of files, the owner of the files, the group of the files, the date of the files, or a version number for a send mail program (lines 36-42, Col. 5)].

Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to have scanning engine for analyzing the vulnerability relating to the software files since one would have been motivated to have a security product (1) function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.) (2) have information contained in the data record reveals a security vulnerability discovered by the module (lines 39-41, Col. 19 from Kingsford et al.), and (3) to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.). Therefore, it would have been obvious to modify Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to obtain the invention as specified in Claim 44.

v. Referring to Claim 45:

As per Claim 45, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the system of claim 39. Gleichauf et al. further disclose the security audit system and the discovery scan, Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses the audit scan as in Claim 1. In addition, Hartley et al. disclose an active scan engine [i.e., **The security system processing module 15 (line13-14, Col. 4)**] operable for selecting, coordinating, and scheduling various scans to be performed on the computer network. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. Kingsford et al., and Hartley et al. to have the active security system processing module managing the scanning processes from Proctor and Gleichauf et al. since one would have been motivated to have a security product function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.) and to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.). Therefore, it would have been obvious to modify

Proctor with Gleichauf et al., Kingsford et al., and Hartley et al. to obtain the invention as specified in Claim 45.

11. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Kingsford et al. (U.S. Patent 6,574,737) as applied to claim 30 above, and further in view of Yang (U.S. Patent 6,467,002)

a. Referring to Claim 33:

As per Claim 33, Proctor, Gleichauf et al., and Kingsford et al. disclose the method of claim 30. In addition, Gleichauf et al. disclose wherein the step of receiving an initial scan comprises:

identifying an operating system and a service for the network element, and identifying at least one vulnerability associated with the network element [**i.e., Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices, and the services available on each device. Additionally, in the embodiment of FIG.1, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (lines 59-65, Col. 5)]. Gleichauf et al. do not**

expressly disclose determining an asset value of the network element from the operating system and the service of the network element. However, Yang discloses a priority assignment module for assigning priority values to various devices in the network environment [i.e., **Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10)].** Proctor, Gleichauf et al., Kingsford et al., and Yang are analogous art because they are from similar technology relating to the computer system linked in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., Kingsford et al. with Yang to have the function of the priority assignment based on the operating system and the services of the network element incorporated into the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang).** Therefore, it would have been obvious to modify Proctor, Gleichauf et

al., and Kingsford et al. with Yang to obtain the invention as specified in Claim 33.

12. Claims 3, 16, 27, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), Kingsford et al. (U.S. Patent 6,574,737), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1, 13, 22, and 39 above, and further in view of Brabson et al. (U.S. Patent 5,715,395).

a. Referring to Claim 3:

As per Claim 3, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. do not explicitly disclose the step of receiving a blackout time during which no audit scan can be scheduled. However, Brabson et al. disclose that network can be scheduled to be unavailable due to the scheduled maintenance and appropriate method would be utilized to provide this information to the network node [i.e., **a particular portion of a network was scheduled to be unavailable for scheduled maintenance it would supply appropriate values for the UNAVAILABILITY PERIOD to the Network nodes. If the UNAVAILABILITY PERIOD information is stored in a table at the originating node the network manager could update the table as required (lines 23-28, Col. 11)**]. Proctor, Gleichauf et al., Kingsford et

al., Hartley et al., and Barbson are analogous art because they are from similar technology relating to the network and computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Brabson et al. to have the schedule module providing time information regarding to scheduled scanning tasks and the blackout time due to network maintenance since one would have been motivated to reduce **the impact of network resource location traffic when resources become unavailable, unreachable, or unlocatable (lines 65-67, Col. 3)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Brabson et al. to obtain the invention as specified in Claim 33.

b. Referring to Claim 16:

As per Claim 16, the rejection of Claim 13 is incorporated. In addition, Claim 16 encompasses limitations that are similar to those of Claim 3. Thus, it is rejected with the same rationale applied against Claim 3 above.

c. Referring to Claim 27:

As per Claim 27, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 22. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. do not explicitly disclose the step of receiving a blackout time during which no audit scan can be scheduled. However,

Brabson et al. disclose that network can be scheduled to be unavailable due to the scheduled maintenance and appropriate method would be utilized to provide this information to the network node for the network manager to be aware [i.e., **Thus, if the network manager was aware that a particular portion of a network was scheduled to be unavailable for scheduled maintenance it would supply appropriate values for the UNAVAILABILITY PERIOD to the Network nodes. If the UNAVAILABILITY PERIOD information is stored in a table at the originating node the network manager could update the table as required (lines 22-28, Col. 11)**]. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Brabson are analogous art because they are from similar technology relating to the network and computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Brabson et al. to have the schedule module providing time information regarding to scheduled scanning tasks and the blackout time due to network maintenance since one would have been motivated to reduce **the impact of network resource location traffic when resources become unavailable, unreachable, or unlocatable (lines 65-67, Col. 3)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Brabson et al. to obtain the invention as specified in Claim 27.

d. Referring to Claim 41:

As per Claim 41, the rejection of Claim 39 is incorporated. In addition, Claim 41 encompasses limitations that are similar to those of Claim 27. Thus, it is rejected with the same rationale applied against Claim 27 above.

13. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Kingsford et al. (U.S. Patent 6,574,737) as applied to claim 30 above, and further in view of Hartley et al. (U.S. Patent 6,889,168) and Brabson et al. (U.S. Patent 5,715,395)

a. Referring to Claim 36:

As per Claim 36, the rejection of Claim 30 is incorporated. In addition, Claim 36 encompasses limitations that are similar to those of Claim 27. Thus, it is rejected with the same rationale applied against Claim 27 above.

14. Claims 6-8, 18, 24 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), Kingsford et al. (U.S. Patent 6,574,737), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1, 13, 22, and 39 above, and further in view of Yang (U.S. Patent 6,467,002).

a. Referring to Claim 6:

As per Claim 6, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. In addition, Gleichauf et al. disclose the step of conducting a discovery scan and a priority engine for prioritizing a plurality of analysis tasks. Gleichauf et al. do not expressly disclose assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network. However, Yang discloses a priority assignment module for assigning priority values to various devices in the network environment [i.e., **Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10).**]. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of**

computer systems and networks (lines 43-46, Col. 1, Yang).

Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 6.

b. Referring to Claim 7:

As per Claim 7, Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Yang disclose the method of claim 6. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Yang do not expressly disclose the asset value is modified based on the audit scan. However, Proctor discloses the audit scan as in Claim 1. In addition, Yang discloses the priorities associated with the devices are subjected to modification [i.e., **Referring again to FIG 2A, in step 250, the priorities are reassigned among the devices (lines 48-49, Col. 6)]**. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer**

systems and networks (lines 43-46, Col. 1, Yang). Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 7.

c. Referring to Claim 8:

As per Claim 8, Proctor and Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. do not expressly disclose the step of receiving a manually selected asset value for the element. However, Yang discloses that the priority value for the network element can be user-selected **[i.e., It is further appreciated that the initial priority order can be user designated (lines 15-17, Col. 6)]**. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine for receiving user input since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shared-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang).**

Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 8.

d. Referring to Claim 18:

As per Claim 18, the rejection of Claim 13 is incorporated. In addition, Claim 18 encompasses limitations that are similar to those of Claim 6. Thus, it is rejected with the same rationale applied against Claim 6 above.

e. Referring to Claim 24:

As per Claim 24, the rejection of Claim 22 is incorporated. Gleichauf et al. further disclose identifying an operating system for the network element **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices (lines 59-61, Col. 5)]**. In addition, Claim 24 encompasses limitations that are similar to those of Claim 4, 5, and 6. Thus, it is also rejected with the same rationale applied against Claim 4, 5, and 6 above.

f. Referring to Claim 40:

As per Claim 40, the rejection of Claim 39 is incorporated. In addition, Claim 40 encompasses limitations that are similar to those of Claim 4, 5,

and 6. Thus, it is also rejected with the same rationale applied against Claim 4, 5, and 6 above.

15. Claims 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), Kingsford et al. (U.S. Patent 6,574,737), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1 and 13 above, and further in view of Yang (U.S. Patent 6,467,002) and Barroux (U.S. Patent 6,220,768).

a. Referring to Claim 10:

As per Claim 10, Proctor, Gleichauf et al., Kingsford et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf, Kingsford et al., and Hartley et al. do not expressly disclose remaining limitations of the claims. However, Gleichauf et al. disclose identifying the function of the network element based on the discovery scan [i.e., **Scan engine 22 can direct request upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices, and services available on each device (lines 59-62, Col. 5)].** Proctor discloses a policy for auditing [i.e., **Audit policy 300 (Fig. 3), which comprises of system audit, object audit, and registry key audit]**. Yang discloses a priority assignment module for assigning

priority values to various devices in the network environment [i.e., **Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2).** Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10)]. Barroux discloses scheduling of tasks required for repetition [**Integrated resource 200 also computes whether tasks need to be repeated and builds an interval schedule for tasks requiring repetition into its schedule (lines 36-38, Col. 4)**]. Proctor, Gleichauf et al., Kingsford et al., Hartley et al., Yang, and Barroux are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., Kingsford et al., Hartley et al. with Yang and Barroux to have the priority values associated to the network elements converted into repetitively scheduled tasks and associated the results with the policy disclosed by Proctor and the role by Gleichauf et al. since one would have been motivated to realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang) and to take advantage of SNMP (Simple Network Management

Protocol) to collect survey information for a TCP/IP network (lines 10-12, Col. 2 from Barroux). Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Kingsford et al., Hartley et al. with Yang and Barroux to obtain the invention as specified in Claim 10.

b. Referring to Claim 19:

As per Claim 19, the rejection of Claim 13 is incorporated. In addition, Claim 19 encompasses limitations that are similar to those of Claim 10. Thus, it is rejected with the same rationale applied against Claim 10 above.

Response to Arguments

1. Applicant's remark, filed on Dec. 14, 2005, has been considered and is found persuasive by the Examiner.
2. Based on the newly amended and added claims, a new ground of rejection on independent claims is made relying on the prior art by Kingsford et al. (U.S. Patent 6,574,737) combining with other previously cited art. Please refer to rejections above.
3. Other dependent claims are rejected based on the combination of the prior art by Kingsford et al. (U.S. Patent 6,574,737) with other previously cited art. Please refer to rejections above.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Fox et al. (U.S. Patent 6,883,101) disclose a method and data processing system assesses the security vulnerability of a network. A system object model database is created and supports the information data requirements of disparate network vulnerability analysis programs. Only the required data from the system object model database representing the network is imported to the programs, which then analyze the network to produce data results from each program. In particular, Fox et al. disclose the fuzzy logic processing in the present invention, which uses evidential reasoning to accumulate evident from the system and tool findings for each criteria, thereby merging the system assessment data into a single point of reference, the conformance of the system to a particular criteria. The accuracy of the result is contingent upon the quantity and quality of the data available and it may be necessary to perform additional refinement on the available data prior to the application of fuzzy logic processing, while also maintaining the probabilistic nature of the data. This refinement uses inference networks and provides a method of reasoning about probability using heuristics, thereby removing the need for extensive a priori knowledge. The relation between the goals and potential security metrics encourages cross fertilization.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS


HOSUK SONG
PRIMARY EXAMINER

Mar. 02, 2006